UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/643,678	08/18/2003	Sundeep M. Bajikar	42P16632	4611

8791 7590 08/06/2008

BLAKELY SOKOLOFF TAYLOR & ZAFMAN LLP
1279 OAKMEAD PARKWAY
SUNNYVALE, CA 94085-4040

EXAMINER	
PATEL, NIRAV B	

ART UNIT	PAPER NUMBER
2135	

MAIL DATE	DELIVERY MODE
08/06/2008	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary	Application No.	Applicant(s)	
	10/643,678	BAJIKAR ET AL.	
	Examiner	Art Unit	
	NIRAV PATEL	2135	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE *3* MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *23 April 2008 (Amendment)*.

2a)☒ This action is **FINAL**. 2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-7 and 9-32* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-7 and 9-32* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☐ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

1. Applicant's amendment filed on April 23, 2008 has been entered. Claims 1-7, 9-32 are pending. Claims 1, 7, 10, 11, 12-15 are amended and Claims 28-32 are newly added by the applicant.

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

2. Claims 1-7, 9, 23, 24, 26-32 are rejected under 35 U.S.C. 103(a) as being unpatentable over Poisner et al (US Patent No. 7,076,669) and in view of Krancher et al (US Patent No. 6,799,237).

As per claim 1, Poisner discloses:

a chipset; an internal component of the computer system [Fig. 1, component 110, 120]; a bus coupled to the chipset to communicate a trusted data cycle to the internal component of the computer system [Fig. 1, col. 3 lines 6-51]; a connector; and a secure docking circuit coupled to the bus and coupled between the bus and the connector (a I/O port or controller) [Fig. 1] to scan for the trusted data cycle detect the trusted data cycle [Fig. 1, col. 4 lines 26-33, 42-51], and provide a filtering mechanism to prevent the trusted data cycle from being provided to a device external to the computer system

through the connector (a I/O port or controller) [Fig. 1, col. 5 lines 6-13]. Poisner teaches the I/O port (connector/controller) as shown in Fig. 1.

Krancher teaches a docking connector, and the docking circuit coupled to the bus and coupled between the bus and the docking connector which provide filtering mechanism to prevent the data from being provided to a device external to the computer system through the docking connector [Fig.1, 3].

Therefore, it would have been obvious to a person of ordinary skill in the art at the time the invention was made to combine Krancher with Poisner, since one would have been motivated to increase functionality of the coupled units [Krancher, col. 1 line 24].

As per claim 2, the rejection of claim 1 is incorporated and Poisner discloses: wherein the bus is a Low Pin Count bus [Fig. 1, col. 3 line 46].

As per claim 3, the rejection of claim 1 is incorporated and Poisner discloses: wherein the component provides protected memory storage [Fig. 1].

As per claim 4, the rejection of claim 1 is incorporated and Poisner discloses: wherein the component provides platform authentication [col. 1 lines 14-20].

As per claim 5, the rejection of claim 1 is incorporated and Poisner discloses: wherein the component maintains a protected path between the chipset and a keyboard [Fig. 1, col. 5 lines 15-18, col. 7 lines 29-32].

As per claim 6, the rejection of claim 1 is incorporated and Poisner discloses: wherein the computer system is a notebook computer [Fig. 1, col. 1 line 15].

As per claim 7, Poisner discloses:

means for transmitting data on a Low Pin Count (LPC) bus [Fig. 1, col. 3 line 46]; and filtering means for scanning for trusted data cycles on the Low Pin Count (LPC) bus and preventing the trusted data cycles on the Low Phi Count (LPC) bus from being accessed by an unauthorized component [Fig. 1, col. 4 lines 26-33, col. 5 lines 6-13].

Poisner teaches preventing the trusted data cycles accessed by an unauthorized component coupled to a controller (or input/output port) [Fig. 1, col. 5 lines 6-13], wherein the filtering means is between the Low Pin Count (LPC) bus and the controller (or input/output port) [Fig. 1, component 120].

Krancher teaches coupling the unauthorized component to a docking connector, filtering means is between the bus and the docking connector [Fig. 1].

Therefore, it would have been obvious to a person of ordinary skill in the art at the time the invention was made to combine Krancher with Poisner, since one would have been motivated to increase functionality of the coupled units [Krancher, col. 1 line 24].

As per claim 9, the rejection of claim 7 is incorporated and Poisner discloses: means for monitoring data cycles on the LPC bus [Fig. 1, col. 4 lines 26-33].

As per claims 23 and 24, the rejection of claim 1 is incorporated and Poisner discloses:

wherein the circuit makes a data cycle that is not a trusted data cycle available to the device external to the computer system [col. 4 lines 57-67, col. 5 line 1].

As per claim 26, the rejection of claim 1 is incorporated and Poisner discloses:

wherein the trusted data cycle begins with a predefined trusted data cycle indicator [Fig. 3 or 4].

As per claim 10, Poisner discloses:

monitoring for communication of trusted data cycles on a bus with a secured docking logic (component 120, which comprises various bus logic, decoder logic) of a computer system, the secured docking logic coupled between the bus and a connector[Fig. 1, col. 3 lines 6-15]; detecting each of the trusted data cycles by detecting a predefined trusted data cycle indicator with the secured docking logic [Fig. 1-4, col. 4 lines 42-59]; and preventing the trusted data cycles from being available to a component external to the computer system with the secured docking logic [col. 5 lines 6-13]. Poisner teaches the I/O port (connector/controller) as shown in Fig. 1.

Krancher teaches a docking connector, and the docking circuit coupled to the bus and coupled between the bus and the docking connector which provide filtering mechanism to prevent the data from being provided to a device external to the computer system through the docking connector [Fig.1, 3].

Therefore, it would have been obvious to a person of ordinary skill in the art at the time the invention was made to combine Krancher with Poisner, since one would have been motivated to increase functionality of the coupled units [Krancher, col. 1 line 24].

As per claim 11, the rejection of claim 10 is incorporated and Poisner discloses:
the trusted data cycles begin with a "0101" value [col. 8 lines 16-17].

As per claim 12, the rejection of claim 10 is incorporated and Poisner discloses:
communicating trusted data cycles between the chipset of the computer system and a first component of the computer system that provides cryptographic capabilities [Fig. 1].

As per claims 13 and 15, the rejection of claims 12 and 14 are incorporated and Poisner discloses:
the communication of the trusted data cycle between the chipset and the first/the second component is in plaintext format [Fig. 1].

As per claim 14, the rejection of claim 10 is incorporated and Poisner discloses:
communicating trusted data cycles between a chipset of the computer system and a second component that provides trusted input capabilities [Fig. 1].

As per claims 16 and 17, the rejection of claim 15 is incorporated and Poisner discloses:

the second component maintains a protected path between the chipset and a keyboard, wherein keystroke data is communicated by the chipset to protected memory and trusted applications [Fig. 1].

As per claim 27, the rejection of claim 10 is incorporated and Poisner discloses:
wherein the circuit makes a data cycle that is not a trusted data cycle available to the device external to the computer system [col. 4 lines 57-67, col. 5 line 1].

As per claim 28, the rejection of claim 1 is incorporated and Poisner discloses:
the trusted data cycle comprises a trusted data cycle indicator and plaintext format data [Fig. 3, 4].

As per claim 29, Poisner discloses:

a chipset; a first internal component to provide at least one hardware cryptographic functionality selected from hardware protected storage, platform binding and platform authentication [Fig. 1, col. 2 lines 56-67, col. 3 lines 1-25]; a second internal component to provide a trusted input capability from a keyboard [Fig. 1]; a bus coupled to the chipset, coupled to the first internal component, and coupled to the second internal component, the bus to communicate a trusted data cycle from the chipset to the first internal component [Fig. 1], a connector; and secured logic coupled between the bus and the connector, the secured logic to block the trusted data cycle from an external device coupled with the connector [Fig. 1, 2, col. 4 lines 26-33, 42-51, col. 5 lines 6-13].

Poisner teaches the I/O port (connector/controller) as shown in Fig. 1.

Krancher teaches a docking connector, and the docking circuit coupled to the bus and coupled between the bus and the docking connector which provide filtering mechanism to prevent the data from being provided to a device external to the computer system through the docking connector [Fig.1, 3].

Therefore, it would have been obvious to a person of ordinary skill in the art at the time the invention was made to combine Krancher with Poisner, since one would have been motivated to increase functionality of the coupled units [Krancher, col. 1 line 24].

As per claim 30, the rejection of claim 29 is incorporated and Poisner discloses: the trusted data cycle comprises a trusted data cycle indicator and data in a plaintext format [Fig. 3, 4].

As per claim 31, the rejection of claim 30 is incorporated and Poisner discloses: the trusted data cycle indicator comprises 0101 [Fig. 3, 4, col. 8 lines 16-17].

As per claim 32, the rejection of claim 30 is incorporated and Krancher discloses: the secured docking logic comprises a circuit [Fig. 1].

3. Claims 18 and 19 are rejected under 35 U.S.C. 103(a) as being unpatentable over Poisner et al [US Patent No. 7,076,669 -- (Poisner '669)] in view of Krancher et al

(US Patent No. 6,799,237) and in view of Poisner [US Pub No. 2004/0268143 -- (Poisner '143)].

As per claim 18, the rejection of claim 12 is incorporated and Poisner '143 discloses: wherein the first component protects secret data of the computer system by encrypting the secret data [paragraph 0029 lines 3-6].

Therefore, it would have been obvious to a person of ordinary skill in the art at the time the invention was made to combine Poisner '143 with Poisner '669 and Krancher, since one would have been motivated to protect data for creating and maintaining a protected operating environment [Poisner '143, paragraph 0029 lines 1-3].

As per claim 19, the rejection of claim 12 is incorporated and Poisner '143 discloses: wherein the secret data is decrypted by hardware of the computer system [paragraph 0029 lines 3-6].

4. Claims 20-22 are rejected under 35 U.S.C. 103(a) as being unpatentable over Poisner et al [US Patent No. 7,076,669 -- (Poisner '669)] in view of Krancher et al (US Patent No. 6,799,237) and in view of Poisner [US Pub No. 2004/0268143 -- (Poisner '143)] and in view of Probst [US Patent No. 5,982,899].

As per claim 20, the rejection of claim 18 is incorporated and Probst discloses:

the first component merges data with configuration values of the computer system [Fig. 1, col. 5 lines 18-39].

Therefore, it would have been obvious to a person of ordinary skill in the art at the time the invention was made to combine Probst with Poisner '669, Krancher and Poisner '143, since one would have been motivated to verify configuration of a computer system and prevent altering or bypassing the computer system information [Probst, col. 4 lines 62-63].

As per claim 21, the rejection of claim 18 is incorporated and Probst discloses:
wherein the first component requests a system identification request [col. 7 lines 13-17, 34-35].

As per claim 22, the rejection of claim 21 is incorporated and Probst discloses:
wherein a trusted third party chip verifies an identification of the computer system and sends a response to the first component [col. 3 lines 49-59, col. 7 lines 36-63].

5. Claim 25 is rejected under 35 U.S.C. 103(a) as being unpatentable over Poisner et al (US Patent No. 7,076,669) and in view of Krancher et al (US Patent No. 6,799,237) and in view of Yanagisawa (US Patent No. 6,519,669).

As per claim 25, the rejection of claim 1 is incorporated and Poisner teaches the circuit blocks the trusted data cycle [Fig. 1, col. 5 lines 9-13].

Yanagisawa teaches the circuit blocks the data cycle from a docking connector [Fig. 1, 2].

Therefore, it would have been obvious to a person of ordinary skill in the art at the time the invention was made to combine Yanagisawa with Poisner and Krancher, since one would have been motivated to control docking and undocking a peripheral device while a computer system is in operation [Yanagisawa, col. 1 lines 9-11].

Response to Amendment

6. Applicant has amended claims 10-15 and added new claims 28-32 which is rejected based on Poisner et al (US Patent No. 7,076,669) and Krancher et al (US Patent No. 6,799,237). See detail rejection above.

Applicant's arguments filed May 23, 2008 have been fully considered but they are not persuasive.

Regarding to applicant argument, "....a secured docking logic that is coupled between the bus and a docking connector; detecting each of trusted data cycle with the secured docking logic; and preventing the trusted data cycle from being available to a component external to the computer system with the secured docking logic ...", Examiner maintains that the prior art Poisner and Krancher teach the claim limitation, since Poisner discloses a computing device as shown in Fig. 1, comprises a token device, processors, a chipset and external devices [Fig. 1]. Processors 110 are coupled

to chipset 120 (secure logic) via a processor bus 164. The chipset includes Input/Output bus interface logic connected to I/O devices via e.g. I/O bus (connector). As shown in Fig. 2, a processor issues a read or write request to chipset. The chipset receives the request from processor via the bus. The chipset decodes the address in the request or decodes the cycle type and determines whether the request is a trusted request. If the request is not a trusted request, the chipset aborts the request. The processor bus interface logic comprises buffers and logic circuits to receive a trusted cycle from a processor and identifies the trusted cycle by identifying a unique value in a field in the trusted cycle. If the address in the trusted cycle is a valid address in token, the trusted cycle or the information in the trusted cycle is sent to I/O bus I/F logic. If the address in the trusted cycle is not a valid address the decoder logic aborts the trust cycle. Therefore, Poisner teaches detecting each of the trusted data cycles with the secured logic (chipset 120 - secured docking logic). Further, the chipset determines the trusted data cycle and prevents from being available to the external component connected to the chipset via bus logic [Fig. 1, 2, col. 3 lines 40-67, col. 4 lines 1-67, col. 5 lines 1-33]. Therefore, Poisner teaches the claim subject matter. In addition, Krancher teaches the logic which couples the bus to the docking connector as shown in Fig. 1, which provides the filtering mechanism to prevent the data from being provided to a device external to the computer system through the docking connector. Therefore, the combination of Poisner and Krancher teaches the claim limitation and the combination is sufficient. The examiner recognizes that obviousness can also be established by combining or modifying the teaching of the prior art to produce the claimed invention

where there is some teaching, suggestion, or motivation to do so found either in the references themselves or in the knowledge generally available to on of ordinary skill in the art. See *In re Fine*, 837 F. 2d 1071, 5 USPQ2d 1596 (Fed. Cir. 1988) and In re Jones, 958 F.2d 347, 21 USPQ 2nd 1941 (Fed. Cir 1992). In fact, Poisner and Krancher do not need to disclose anything over and above the invention as claimed in order to render it unpatentable or anticipate. A recitation of the intended use of the claimed invention must result in structural difference between the claimed invention and the prior art in order to patentably distinguish the claimed invention from the prior art. If the prior art structure is capable of performing the intended use, then it meets the claimed limitations.

Conclusion

7. Accordingly, **THIS ACTION IS MADE FINAL**. See MPEP § 706.07(a). Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of

the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the date of this final action.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Nirav Patel whose telephone number is 571-272-5936. If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Kim Vu can be reached on 571-272-3859. The fax and phone numbers for the organization where this application or proceeding is assigned is 571-273-8300. Any inquiry of a general nature or relating to the status of this application or proceeding should be directed to the receptionist whose telephone number is 571-272-2100.

NBP
7/30/08
/KimYen Vu/

Supervisory Patent Examiner, Art Unit 2135